

# FINITE ORDER ELEMENTS IN THE INTEGRAL SYMPLECTIC GROUP

KUMAR BALASUBRAMANIAN, M. RAM MURTY,  
AND KARAM DEO SHANKHADHAR

## ABSTRACT

For  $g \in \mathbb{N}$ , let  $G = \text{Sp}(2g, \mathbb{Z})$  be the integral symplectic group and  $S(g)$  be the set of all positive integers which can occur as the order of an element in  $G$ . In this paper, we show that  $S(g)$  is a bounded subset of  $\mathbb{R}$  for all positive integers  $g$ . We also study the growth of the functions  $f(g) = |S(g)|$ , and  $h(g) = \max\{m \in \mathbb{N} \mid m \in S(g)\}$  and show that they have at least exponential growth.

## 1. INTRODUCTION

Given a group  $G$  and a positive integer  $m \in \mathbb{N}$ , it is natural to ask if there exists  $k \neq 1 \in G$  such that  $o(k) = m$ , where  $o(k)$  denotes the order of the element  $k \in G$ . In this paper, we make some observations about the collection of positive integers which can occur as orders of elements in  $G = \text{Sp}(2g, \mathbb{Z})$ . Before we proceed further we set up some notation and briefly mention the problems studied in this paper.

Let  $G = \text{Sp}(2g, \mathbb{Z})$  be the group of all  $2g \times 2g$  matrices with integral entries satisfying

$$A^\top J A = J$$

where  $A^\top$  is the transpose of the matrix  $A$  and  $J = \begin{pmatrix} 0_g & I_g \\ -I_g & 0_g \end{pmatrix}$ .

Throughout we write  $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ , where  $p_i$  is a prime and  $\alpha_i > 0$  for all  $i \in \{1, 2, \dots, k\}$ . We also assume that the primes  $p_i$  are such that  $p_i < p_{i+1}$  for  $1 \leq i < k$ . We write  $\pi(x)$  for the number of primes less than or equal to  $x$ . Also for  $A \in G$  we let  $o(A)$  denote the order of  $A$ . We let  $\phi$  denote the Euler's phi function. It is a well known fact that the function  $\phi$  is multiplicative, i.e.,  $\phi(mn) = \phi(m)\phi(n)$  if  $m, n$  are relatively prime and

---

Research of Kumar Balasubramanian was supported by DST-SERB Grant: YSS/2014/000806.

Research of M. Ram Murty was partially supported by an NSERC Discovery grant.

satisfies  $\phi(p^\alpha) = p^\alpha(1 - \frac{1}{p})$  for all primes  $p$  and positive integer  $\alpha \in \mathbb{N}$  (see [2] for a proof). Let

$$S(g) = \{m \in \mathbb{N} \mid \exists A \neq 1 \in G \text{ with } o(A) = m\}.$$

In this paper we show that  $S(g)$  is always a bounded subset of  $\mathbb{R}$  for all positive integers  $g$ . Once we know that  $S(g)$  is a bounded set, it makes sense to consider the functions  $f(g) = |S(g)|$ , where  $|S(g)|$  is the cardinality of  $S(g)$  and  $h(g) = \max\{m \mid m \in S(g)\}$ , i.e.,  $h(g)$  is the maximal possible (finite) order in  $G = \text{Sp}(2g, \mathbb{Z})$ . We show that the functions  $f$  and  $h$  have at least exponential growth.

The above problem derives its motivation from analogous problems from the theory of mapping class groups of a surface of genus  $g$ . We know that given a surface  $S_g$  of genus  $g$ , there is a surjective homomorphism  $\psi : \text{Mod}(S_g) \rightarrow \text{Sp}(2g, \mathbb{Z})$ , where  $\text{Mod}(S_g)$  is the mapping class group of  $S_g$ . It is a well known fact that for  $f \in \text{Mod}(S_g)$  ( $f \neq 1$ ) of finite order, we have  $\psi(f) \neq 1$ . Let  $\tilde{S}(g) = \{m \in \mathbb{N} \mid \exists f \neq 1 \in \text{Mod}(S_g) \text{ with } o(f) = m\}$ . The set  $\tilde{S}(g)$  is a finite set and it makes sense to consider the functions  $\tilde{f}(g) = |\tilde{S}(g)|$  and  $\tilde{h}(g) = \max\{m \in \mathbb{N} \mid m \in \tilde{S}(g)\}$ . It is a well known fact that both these functions  $\tilde{f}$  and  $\tilde{h}$  are bounded above by  $4g + 2$ . We refer the reader to [5] for an excellent introduction to the mapping class group and the proofs of some of these facts.

## 2. SOME RESULTS WE NEED

In this section we mention a few results that we need in order to prove the main results in this paper.

**Proposition 2.1** (Bürgisser). *Let  $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ , where the primes  $p_i$  satisfy  $p_i < p_{i+1}$  for  $1 \leq i < k$  and where  $\alpha_i \geq 1$  for  $1 \leq i \leq k$ . There exists a matrix  $A \in \text{Sp}(2g, \mathbb{Z})$  of order  $m$  if and only if*

- a)  $\sum_{i=2}^k \phi(p_i^{\alpha_i}) \leq 2g$ , if  $m \equiv 2 \pmod{4}$ .
- b)  $\sum_{i=1}^k \phi(p_i^{\alpha_i}) \leq 2g$ , if  $m \not\equiv 2 \pmod{4}$ .

*Proof.* See corollary 2 in [1] for a proof. □

**Proposition 2.2** (Dusart). *Let  $p_1, p_2, \dots, p_n$  be the first  $n$  primes. For  $n \geq 9$ , we have*

$$p_1 + p_2 + \dots + p_n < \frac{1}{2}np_n.$$

*Proof.* See theorem 1.14 in [3] for a proof.  $\square$

**Proposition 2.3** (Dusart). *For  $x \geq 2$ ,  $\pi(x) \leq \frac{x}{\log x} \left(1 + \frac{1.2762}{\log x}\right)$ . For  $x \geq 599$ ,  $\pi(x) \geq \frac{x}{\log x} \left(1 + \frac{1}{\log x}\right)$ .*

*Proof.* See theorem 6.9 in [4] for a proof.  $\square$

**Proposition 2.4** (Dusart). *For  $x \geq 2973$ ,*

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) > \frac{e^{-\gamma}}{\log x} \left(1 - \frac{0.2}{(\log x)^2}\right).$$

*where  $\gamma$  is the Euler's constant.*

*Proof.* See theorem 6.12 in [4] for a proof.  $\square$

**Proposition 2.5** (Rosser). *For  $x \geq 55$ , we have  $\pi(x) > \frac{x}{\log x + 2}$ .*

*Proof.* See theorem 29 in [6] for a proof.  $\square$

### 3. MAIN RESULTS

In this section we prove the main results of this paper. To be more precise, we prove the following.

- a)  $S(g)$  is a bounded subset of  $\mathbb{R}$ .
- b)  $f(g) = |S(g)|$  has at least exponential growth.
- c)  $h(g) = \max\{m \mid m \in S(g)\}$  has at least exponential growth.

3.0.1. *Boundedness of  $S(g)$ .* For each  $g \in \mathbb{N}$ , let  $S(g) = \{m \in \mathbb{N} \mid \exists A \neq 1 \in G \text{ with } o(A) = m\}$ . In this section we show that  $S(g)$  is a bounded subset of  $\mathbb{R}$ .

Let  $m = p_1^{\alpha_1} \dots p_k^{\alpha_k} \in S(g)$ . Suppose  $p_i > 2g+1$  for some  $i \in \{1, 2, \dots, k\}$ . This would imply that  $\phi(p_i^{\alpha_i}) = p_i^{\alpha_i-1}(p_i-1) > 2g$ , which contradicts proposition 2.1. It follows that all primes in the factorization of  $m$  should be  $\leq 2g+1$  and hence  $k \leq g+1$ .

**Theorem 3.1.** *For  $g \in \mathbb{N}$ ,  $S(g)$  is a bounded subset of  $\mathbb{R}$ .*

*Proof.* For  $g \in \mathbb{N}$ , fix  $k = \pi(2g+1)$  and  $P = \{p_1, p_2, \dots, p_k\}$  be the set of first  $k$  primes arranged in increasing order. The prime factorization of any  $m \in S(g)$  involves primes only from the set  $P$ . The total number of non-empty subsets of  $P$  is  $2^k - 1$ . Let us denote the collection of these subsets

of  $P$  as  $\{P_1, P_2, \dots, P_{2^k-1}\}$ . For  $1 \leq a \leq 2^k - 1$ , let  $P_a$  denote the subset  $\{q_1, q_2, \dots, q_n\}$  of  $P$ , where  $n = n(P_a)$  is the number of primes in the subset  $P_a$ . For a fixed  $a$  (and hence fixed  $P_a$ ), define

$$m_a = m_a(\alpha_1, \dots, \alpha_n) = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_n^{\alpha_n},$$

$$r_a = r_a(\alpha_1, \dots, \alpha_n) = \sum_{i=1}^n q_i^{\alpha_i} \left(1 - \frac{1}{q_i}\right),$$

where  $\alpha_i > 0$ . The key idea of the proof is to maximize the function  $m_a$  considered as a function of the real variables  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  with respect to the inequality constraint  $r_a \leq 2g + 1$ . We let  $M_a$  denote this maximum. Using the Lagrange multiplier method we see that the function  $m_a$  attains the maximum  $M_a$  precisely when  $q_i^{\alpha_i} (1 - \frac{1}{q_i}) = q_j^{\alpha_j} (1 - \frac{1}{q_j})$  for all  $1 \leq i, j \leq n$ . Under the above condition, the constraint  $r_a \leq 2g + 1$  gives us  $q_i^{\alpha_i} (1 - \frac{1}{q_i}) \leq \frac{2g+1}{n}$ , for any  $1 \leq i \leq n$ . Now

$$m_a(\alpha_1, \alpha_2, \dots, \alpha_n) = \frac{q_1^{\alpha_1} (1 - \frac{1}{q_1}) q_2^{\alpha_2} (1 - \frac{1}{q_2}) \dots q_n^{\alpha_n} (1 - \frac{1}{q_n})}{\prod_{i=1}^n \left(1 - \frac{1}{q_i}\right)}.$$

From this it follows that for  $1 \leq a \leq 2^k - 1$ ,

$$M_a = \frac{\left(q_1^{\alpha_1} (1 - \frac{1}{q_1})\right)^n}{\prod_{i=1}^n \left(1 - \frac{1}{q_i}\right)} \leq \frac{\left(\frac{2g+1}{n}\right)^n}{\prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)}.$$

Therefore, for  $m \in S(g)$ , we have

$$\begin{aligned} m &\leq \max_{1 \leq a \leq 2^k-1} M_a \\ &\leq \frac{\max_{1 \leq a \leq 2^k-1} \left(\frac{2g+1}{n}\right)^n}{\prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)} \\ &\leq \frac{e^{\frac{2g+1}{e}}}{\prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)} \end{aligned}$$

In the above computation, we have used the fact that for  $x > 0$ ,  $\left(\frac{2g+1}{x}\right)^x$  attains the maximum when  $x = (2g + 1)/e$ .

Observing that  $\prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) \geq \frac{1}{2} \frac{2}{3} \left(\frac{4}{5}\right)^{\pi(2g+1)-2}$ , we have

$$m \leq 3(5/4)^{\pi(2g+1)-2} e^{\frac{2g+1}{e}} \leq 3e^{\left(\frac{2g+1}{e} + g - 1\right)} \leq 3e^{3g}.$$

□

**Corollary 3.2.** For  $g \in \mathbb{N}$ ,  $f(g) \leq h(g) \leq 3e^{3g}$ .

*Proof.* For  $m \in S(g)$ , we have  $m \leq 3e^{3g}$ . The result follows. □

*Remark 3.3.* Upper bound for  $S(g)$  for  $g \geq 1486$ : The bound obtained in theorem 3.1 is an absolute upper bound for  $S(g)$ . For  $g \geq 1486$ , we can improve the above upper bound as follows: Using proposition 2.4, we get

$$\prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) > \frac{1}{2} \frac{e^{-\gamma}}{\log(2g+1)}.$$

Therefore it follows that for  $m \in S(g)$ , we have

$$m \leq \frac{e^{\frac{2g+1}{e}}}{\prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)} \leq 2e^{\gamma} \log(2g+1) e^{\frac{2g+1}{e}}.$$

**3.0.2. Growth of  $f(g)$  and  $h(g)$ .** In the previous section, we computed an upper bound for the functions  $f(g)$  and  $h(g)$ . In this section we show that  $f(g)$  and  $h(g)$  have at least exponential growth.

**Lemma 3.4.** For  $x \geq 23$ , we have

$$\sum_{p \leq x} p < \frac{1}{2} x \pi(x)$$

where the sum is over all primes  $p \leq x$ .

*Proof.* Let  $n$  be such that  $p_n \leq x < p_{n+1}$ , where  $p_n$  denotes the  $n^{\text{th}}$  prime number. It follows from proposition 2.2, that for  $x \geq 23$ , we have

$$\sum_{p \leq x} p = \sum_{p \leq p_n} p < \frac{1}{2} n p_n \leq \frac{1}{2} \pi(x) x.$$

□

Before we proceed further, we set up some notation which we need in the following results.

Let  $K(\geq e) \in \mathbb{N}$  be such that for  $\sqrt{K \log K} \geq 23$ .

**Lemma 3.5.** For  $g \geq K$ ,  $\pi(\sqrt{g \log(g)}) < \frac{3\sqrt{g \log(g)}}{\log(g \log(g))}$ .

*Proof.* For  $y > 1$ , we have  $\pi(y) < \frac{y}{\log(y)} \left(1 + \frac{3}{2\log(y)}\right)$  (see proposition 2.3). Using this estimate we get,

$$\begin{aligned} \pi(\sqrt{g \log(g)}) &< \frac{\sqrt{g \log(g)}}{\log(\sqrt{g \log(g)})} \left(1 + \frac{3}{2\log(\sqrt{g \log(g)})}\right) \\ &\leq \frac{\sqrt{g \log g}}{\log(\sqrt{g \log g})} \left(1 + \frac{3}{2\log 23}\right) \\ &= \frac{3\sqrt{g \log(g)}}{\log(g \log(g))}. \end{aligned}$$

□

**Lemma 3.6.** Let  $x = \sqrt{g \log(g)}$  and  $m = m(g) = \prod_{p \leq x} p$ . Then for  $g \geq K$ , we have  $m \in S(g)$ .

*Proof.* By proposition 2.1, it is enough to show that  $\beta = \sum_{2 \neq p \leq x} (p-1) \leq 2g$ .

Using lemma 3.4 and lemma 3.5, we have

$$\begin{aligned} \beta &< \sum_{p \leq x} p < \frac{1}{2}(\sqrt{g \log(g)})\pi(\sqrt{g \log(g)}) \\ &< \frac{3}{2} \frac{g \log(g)}{\log(g \log(g))} = \frac{3}{2}g. \end{aligned}$$

□

For  $g \geq K$ , let  $A(g) = \{p \in \mathbb{N} \mid p \leq \sqrt{g \log(g)}\}$  and  $m = m(g)$  be as above. If  $d$  is any divisor of  $m$ , then it is easy to see that  $d \in S(g)$ . Also it is clear that the divisors  $d$  of  $m$  are in bijection with the number of subsets of  $A(g)$ . Since any divisor  $d$  of  $m$  is an element in  $S(g)$  and the number of divisors correspond bijectively with subsets of  $A(g)$ , it follows that  $f(g) = |S(g)| \geq 2^{\pi(\sqrt{g \log(g)})}$  (since number of subsets of  $A(g) = 2^{\pi(\sqrt{g \log(g)})}$ ).

We will now show that  $|S(g)| > e^{\frac{1}{4}\sqrt{\frac{g}{\log(g)}}}$  from which it follows that the function  $f(g) = |S(g)|$  has at least exponential growth.

**Theorem 3.7.** *Let  $L \in \mathbb{N}$  such that  $\sqrt{L \log L} \geq 55$ . Then  $f(g) = |S(g)| > e^{\frac{1}{4}\sqrt{\frac{g}{\log(g)}}}$  for all  $g \geq L$ .*

*Proof.* From proposition 2.5, we have for all  $g \geq L$ ,

$$\frac{\sqrt{g \log(g)}}{\log(g \log(g))} < \pi(\sqrt{g \log(g)}).$$

From this it follows that for all  $g \geq L$ , we have

$$f(g) \geq 2^{\pi(\sqrt{g \log(g)})} > 2^{\frac{\sqrt{g \log(g)}}{\log(g \log(g))}} > 2^{\frac{1}{2}\sqrt{\frac{g}{\log(g)}}} > e^{\frac{1}{4}\sqrt{\frac{g}{\log(g)}}}.$$

□

**Corollary 3.8.** *Let  $L \in \mathbb{N}$  be as in the above theorem. Then  $h(g) > e^{\frac{1}{4}\sqrt{\frac{g}{\log(g)}}}$  for all  $g \geq L$ .*

*Proof.* Since  $h(g) \geq f(g)$ , the result follows. □

*Remark 3.9.* For  $g \log g \geq (599)^2$ , we can improve the above lower bound  $e^{\frac{1}{4}\sqrt{\frac{g}{\log g}}}$  to  $e^{\sqrt{\frac{g}{4 \log g}}}$  by using proposition 2.3.

## REFERENCES

1. B. Bürgisser, *Elements of finite order in symplectic groups*, Arch. Math. (Basel) **39** (1982), no. 6, 501–509. MR 690470 (85b:20062)
2. David M. Burton, *Elementary number theory*, Allyn and Bacon Inc., Boston, Mass., 1980, Revised printing. MR 567137 (81c:10001b)
3. Pierre Dusart, *Autour de la fonction qui compte le nombre de nombres premiers*, Thesis (1998).
4. ———, *Estimates of some functions over primes without R.H.*, arxiv:1002.0442v1.
5. Benson Farb and Dan Margalit, *A primer on mapping class groups*, Princeton Mathematical Series, vol. 49, Princeton University Press, Princeton, NJ, 2012. MR 2850125
6. Barkley Rosser, *Explicit bounds for some functions of prime numbers*, Amer. J. Math. **63** (1941), 211–232. MR 0003018

KUMAR BALASUBRAMANIAN, DEPARTMENT OF MATHEMATICS, IISER BHOPAL, BHOPAL, MADHYA PRADESH 462066, INDIA

*E-mail address:* bkumar@iiserb.ac.in

M. RAM MURTY, DEPARTMENT OF MATHEMATICS AND STATISTICS, QUEENS UNIVERSITY, KINGSTON, ONTARIO K7L 3N6, CANADA

*E-mail address:* murty@mast.queensu.ca

KARAM DEO SHANKHADHAR, DEPARTMENT OF MATHEMATICS, IISER BHOPAL, BHOPAL, MADHYA PRADESH 462066, INDIA

*E-mail address:* karamdeo@iiserb.ac.in